Coordinating health & health care for a thriving Kansas

KHPA™ KANSAS HEALTH POLICY AUTHORITY

Kansas Health Policy Authority Operational Policy

Title: Computer Security Incident Policy

Number: POL-IT:2008-18
Effective date: 10-03-08
Date Revised: None
Date of Annual Review: None
Authority: POL-EX:2006-01

CATEGORY
Information Technology

SUBJECT
Information Technology Security

BACKGROUND
Kansas Health Policy Authority is highly dependent upon information technology. Much of the information the agency deals with is of a highly sensitive nature and is protected by federal regulation. It is mission critical that each employee and others with access to this information be held responsible to protect this information.

POLICY STATEMENT
All persons with access to electronic Protected Health Information (ePHI) and Personally Identifiable Information (ePII) are accountable to practice due diligence to protect the confidentiality, integrity and availability of that information. Any incident which affects the integrity or security of the KHPA Information Technology System will be reviewed by the Information Security Officer (ISO). Incidents may affect IT system wide or applications only. Examples of such incidents include but are not limited to the following:

- Accidental disclosure of electronic protected health information (ePHI) or electronic Personally Identifiable Information (ePII).
- Purposeful disclosure of ePHI or ePII.
- Access to KHPA owned, managed or maintained computers by any person not authorized such access, including unauthorized physical access to KHPA facilities.
- Infection of KHPA owned, managed or maintained computers by viruses, worms, trojan horses or other malicious software.
- Denial of service attacks on KHPA networks and computers.
- Social engineering aimed at gaining knowledge that will allow access to KHPA IT System to occur.
- Improper, illegal or unethical use of KHPA owned, managed or maintained computers by KHPA employees, agents, associates, representatives, interns,

contractors, temporary employees, auditors, assignees, other designees or vendors.

- The theft or accidental loss of KHPA owned, managed or maintained computers or data storage equipment, such as laptops being lost or stolen from an employee's car or home.

ePHI is all PHI in electronic format and whether in transit or at rest. PHI is defined in the Final Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA) as follows:

Protected Health Information is any individually identifiable health information held or transmitted by KHPA or other covered entity in any form or media. Individually identifiable health information is information which relates to:

1. Relates to the past, present or future physical or mental health or condition of an individual, the provision of healthcare to an individual and
2. Which identifies the individual, or
3. With respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

Malicious software is defined as a virus, worm, trojan horse or other code that infects a computer or other component of the network infrastructure.

Refer to Computer Security Incident Response and Reporting for instructions on how to report security incidents.

SPONSOR/CONTACT
Chief Operations Officer